United States Senate
Republican Policy Committee
Jon Kyl, Chairman
347 Russell Senate Office Building
Washington, DC 20510
202-224-2946
http://rpc.senate.gov

September 6, 2006

Post-9/11 Port Security: Countering Disruption to the Homeland Competently and Judiciously

Executive Summary

- The August 10 aviation terrorist plot in Britain underscores Congress's responsibility to address security at *all* of the nation's portals, including shipping ports.

- Some policymakers have called for immediate *physical* inspections of all cargo containers.
  - Some 11 million containers move through U.S. shipping ports yearly, and there are some 2,100 federal maritime cargo inspectors. That averages to 22 containers per inspector per day.
  - Compare that to a RAND Corporation study that suggests it would take 15 to 20 inspectors an average of four hours to inspect a suspicious container.
  - Even if 100 percent physical inspections could be implemented, the cost would be prohibitive.

- Is 100 percent x-ray *scanning* of containers imported to the U.S. viable?
  - Images provided by current technology can only tell the inspector so much (see pictures on page 6 and 7).
  - Commercial traffic must slow to allow scanning *and* analysis.
  - Add to this the fact that more than 700 ports import cargo to the U.S.

- A *prudent response* – utilize different layers of screening in line with available resources, and upgrade these processes as new technology make more rigorous inspections feasible.

- Currently, DHS already has the following programs:
  - importers provide advance manifests of all U.S.-bound cargo;
  - the Container Security Initiative at some foreign ports (constituting 75 percent of importing to the U.S.) allows U.S. inspectors to screen containers abroad; and
  - DHS has partnered with private importers to approve security plans for supply chains.

- Generally, what else should be done:
  - supporting *new* stages in a layered inspection process *as new technology develops*, and as new methods and programs prove useful;
  - encouraging ports to acquire more non-intrusive inspection machines and reasonable footprint space at major ports;
  - supporting the negotiation of agreements with foreign countries to allow DHS inspectors access to U.S.-bound containers at more foreign ports; and
  - a physical walk-through of security plans of private importers.

Introduction

Since the airborne terrorist attacks of September 11, 2001 ("9/11"), policymakers have recognized the possibility that our nation's shipping ports, too, may be terrorist targets. The revelation on August 10 that a major terrorist plot against the United States was in the works by British nationals who allegedly were planning to exploit security flaws in aviation screening only underscores Congress's responsibility to address security issues at *all* of the nation's portals, including shipping ports.[1]

Based on the known history of actions by groups such as al Qaeda, it seems likely that terrorists will attempt to exploit targets other than airliners – particularly those U.S. portals through which weapons and personnel can travel. One catastrophic scenario that has been pondered, for example, is that terrorists may attempt to place a weapon of mass destruction (e.g., chemical and biological weapon, or a nuclear "dirty bomb") on an inbound cargo container and either move the container to a targeted location or detonate it at a major U.S. harbor.

The natural reaction to such a threat is to call for immediate and rigorous inspections of all cargo containers. However, the reality of the importation regime in the United States places great logistical, practical, and resource restraints on implementing such a policy. Although it is a worthy goal, physical inspections of every cargo container entering the United States would be impermissibly expensive and practically impossible given present technology. Even with promising, developing technology that allows non-intrusive inspection of cargo containers, immediate implementation of such a massive inspective regime may be impractical in the short run. In FY 2004, 23.5 million containers moved through U.S. ports of entry, of which nearly half were maritime containers entering on ships at U.S. ports.[2]

Instead, a prudent response to such a terrorist threat is to utilize different layers of screening in line with available technology and resources, and upgrade these processes as new technology, resources, and reduced costs make more rigorous inspections feasible. In fact, that is the policy that the Administration, with Congress's oversight, has implemented since 9/11. Congress should continue to be supportive of such an approach, and should be vigilant in ensuring that policies and pursuits stay abreast of technological improvements.

---

[1] This paper is limited in scope to maritime container security, although air cargo remains a concern as well. See Andy Pasztor, "Air Cargo Still Largely Unchecked," *Wall Street Journal*, August 15, 2006, p. B1. For a cost estimate of such a catastrophe, see Bruce Mongelluzzo, "Nuclear Attack on LA-LB would cause $1 Trillion Economic Impact," *Journal of Commerce Online*, August 17, 2006, citing RAND Center for Terrorism Risk Management Policy.

[2] Maritime Containers entering the U.S. totaled 11.3 million in FY2005 (CBP Annual Report). Approximately 60,000 port calls are made each year, constituting 1,258,240,424 metric tons of cargo. U.S. Maritime Administration, "Vessel Calls at U.S. Ports, 2004," July 2005 (available at http://www.marad.dot.gov/MARAD_statistics/vcalls2004.pdf) and "U.S. Customs Ports 1997-2005" (available at http://www.marad.dot.gov/MARAD_statistics/index.html#Economic%20Analysis).

Continuing Efforts to Secure Ports Since 9/11

The federal government has completed an enormous amount of work to strengthen U.S. ports since 9/11, including passage of the Maritime Transportation Security Act (MTSA) in 2002, and implementation here and abroad of programs governed by the re-tooled U.S. Customs & Border Protection (CBP).

MTSA (P.L. 107-295) authorized several programs to be implemented by the Coast Guard (now part of the Department of Homeland Security) including: (1) creation of a secure universal identification card for legitimate port facility personnel, (2) requiring assessments of facility and vessel vulnerability, (3) creation of maritime transportation security and response plans, (4) equitable allocation of grants for port security, (5) creation of a long-range vessel tracking system, (6) creation of seafarer identification, (7) evaluating inter-modal transportation, (8) developing performance standards for physical security of shipping and, (9) requiring advance notification of manifest cargo information.

Cargo inspection has warranted particular attention since 9/11, and the Department of Homeland Security (DHS) has pursued what is termed a "layered inspections" regime. Under this approach, importers must provide advance manifests of all cargo containers brought into the United States. In this layer, DHS will run computer algorithms using various risk factors associated with the cargo listed in each cargo manifest.[3] For example, a well-known importer may have its risk score lowered, while an incomplete or inconsistent manifest will be scrutinized more heavily when the cargo reaches the U.S. port. The algorithm computer program, called the Automated Targeting System (ATS), utilizes 240 factors or rules in determining which containers will be considered high risk and targeted for physical and non-intrusive scanning when reaching an American port.[4] The intelligence community also contributes information to the targeted inspections system.

While the ATS is certainly an intelligent method to provide risk assessments, the weakness is that the system is dependent on the accuracy of the cargo manifest. That manifest is provided by the importer and not often confirmed by officials before leaving the foreign port.[5] One solution to this problem is to inspect cargo as it is loaded on ships at foreign ports. Depending on the country, however, foreign port officials may be susceptible to bribes and undue influence from organized crime, and may be less than

[3] CBP receives 98 percent of all maritime cargo manifests before they arrive in the U.S. CBP, "Performance and Accountability Report," FY2005, p. 9. The House report for its latest DHS appropriations bill (H.R. 5441) requires that "all inbound cargo is screened through" ATS (p. 9).
[4] See Testimony of Richard Stana, Government Accountability Office, House of Representatives Committee on Energy and Commerce, March 31, 2004, GAO-04-557T, and Customs and Border Protection briefing materials, June 23, 2006 (available upon request).
[5] Theoretically, any terrorist could type up a false manifest and hide ownership of the cargo through a series of sales between shell companies; bills of lading, indicating ownership of a cargo container, are regularly bought and sold several times during the time cargo is transported between ports. However, CBP and ATS will target manifests that indicate ownership by an unknown or unfamiliar entity.

completely reliable in fully inspecting cargo on behalf of U.S. officials. In an attempt to address these issues, CBP has negotiated agreements with 44 foreign ports, constituting 75 percent of importations to the United States,[6] to allow for small contingents of CBP agents to inspect cargo as it is loaded onto ships. This program is called the Container Security Initiative (CSI).

The CBP contingents are too small (due to resource constraints) to inspect all cargo, so they engage in targeted inspections. These officials are dependent on the good will of their foreign hosts in their ability to target cargo and physically inspect them, but cooperative protocols have been worked out to inspect and offload containers. Of great concern to foreign officials is that inspections would slow the flow of commerce. Any slowdown costs money for the private traders, domestic commercial interests, and the port itself.

In an attempt to mitigate some of these problems and make the most efficient use of all its personnel resources, CBP has tried to encourage private importers to beef up the security of their own supply chain. This program is called the Customs Trade Partnership Against Terrorism, or CTPAT.[7] At present, CBP treats every importer differently, under different standards depending on local conditions, and very few security plans are physically verified by CBP; however, CBP has plans to make regular on-site verification of security plans in the near future.[8] Nevertheless, companies that follow a CBP-approved supply chain security plan obtain a lower risk score when it comes to the container inspections algorithm. In theory, if a company can secure the supply chain, then no terrorist can slip in contraband with that importer's goods in a container bound for the United States. While this is just another layer in the multilayered approach that CBP is currently employing, it is an important step towards added container security.

The Challenges Associated with 100 Percent Inspection

With many security cavities in maritime cargo inspection, some policymakers have argued that 100 percent of all cargo should be inspected before or at arrival in the United States. Before addressing this proferred solution, it is important to recognize that there may be some confusion and differences in what various parties mean when they call for "100 percent inspection."

Physical Inspection

If a policymaker means that he or she favors *physical* inspection of all cargo containers, several factors impede the implementation of such a policy. First, consider

[6] Government Accountability Office, "Container Security: Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts," April 2005, GAO-05-557. Customs and Border Protection briefing materials for Republican staff, June 23, 2006 (available upon request). CBP, "Performance and Accountability Report," FY2005, p. 25.
[7] CBP, "Securing the Global Supply Chain," available at http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/.
[8] Government Accountability Office, "Homeland Security: Key Cargo Security Programs can be Improved," GAO-05-466T.

that some 11.3 million maritime containers enter the United States through shipping ports per year.[9] CBP currently employs 2,100 maritime cargo inspectors to examine 226,000 per week. That means that each inspector would have to single-handedly inspect 22 containers each day (based on a 5-day, 50-week work year). Compare that number to a RAND Corporation study that suggests that to open, remove, and inspect the cargo of a suspicious container could take as long as four hours using 15 to 20 inspectors.[10] And, it is not even clear if that estimate of time includes repacking the container to its previous seaworthy condition – a challenge in itself. Recall that this process includes cutting seals and bolts, separating and inspecting the often tightly packed contents, fitting all the contents back into the container, re-sealing the doors, and moving the cargo along. Further complicating the process is the fact that containers undergoing inspection would need to be moved to special facilities to handle physical inspections of the cargo because most ports have very little unassigned dock space, and so could not handle such a process alongside the ship.[11]

Non-Intrusive Inspection

Policymakers may mean "100 percent inspection" to include non-intrusive inspection as well. CBP has employed x-ray scanning, gamma ray scanning,[12] and radiation detection technologies[13] in a variety of settings. For example, the Vehicle and Cargo Inspections System (VACIS) gamma-ray machines are mobile or stationed machines with a large arm employed right at the dock. These machines can either be moved over a cargo container, or the container can be placed on trucks as they pass under the VACIS arm. A CBP inspector looks at a video screen, and a black and white image of container content outlines appear. If the manifest describes the container as holding tables, for example, an outline of tables should appear on the screen. If a different image appears, a CBP inspector may mark the container for physical inspection.[14]

There are obvious weaknesses in the VACIS system, including the limitation that the image it provides can only tell the inspector so much. That is, tables may appear as one large mass because they are packed with other furniture parts, or tightly packed shoes may not show an outline of shoes. Also, containers passing through such a system can only travel at a very slow rate of speed in order for an image to appear. Further, as the

[9] Customs and Border Protection, "On a Typical Day, U.S. Customs and Border Protection," February 2006 (Note that the annual figure is 23.5 million when including truck, rail, and maritime cargo containers; based on FY04 data). Available upon request. Maritime containers entering the U.S. totaled 11.3 million in FY2005 (CBP Annual Report).

[10] Inspections statistics provided by Customs and Border Protection. Susan Martonosi, et al, "Evaluating the Viability of 100 per cent container inspection at America's Ports," RAND Corp., p. 221. Note, however, that in some instances, physical inspection can be abbreviated by "tunneling" through parts of a container and looking at some of the contents or sending in a dog to detect contraband.

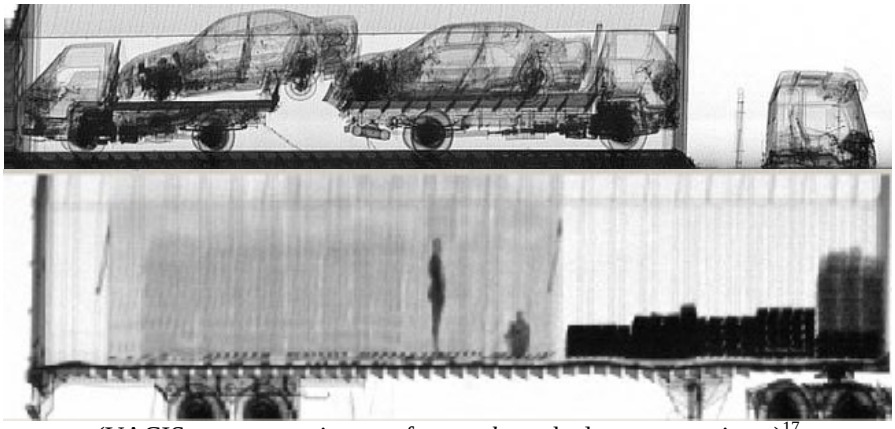
[11] The House report for its latest DHS appropriations bill (H.R. 5441) requires that CBP double the percentage of containers actually inspected (p. 9).

[12] Gamma-ray non-intrusive inspection machines can produce images faster than X-ray machines; however, the images have less resolution, especially for densely-packed containers.

[13] More information on radiation portal monitors is available at www.saic.com/products/security/at-900s.

[14] According to CBP, "Performance and Accountability Report," FY2005, p. 31, about 8.1 percent of maritime cargo containers were examined using non-intrusive technology, such as VACIS.

image appears, it can take an inspector up to 15 minutes to evaluate the image, and there may be considerable problems with scanning fatigue (inspectors cannot remain focused while watching hundreds of images in a given day). At this rate, a massive backlog of cargo would be sitting on the docks and consumer costs would mount if 100 percent vetted scanning were required.[15] Given all of this, it may not be wise to use limited personnel resources on all containers rather than on containers that should raise suspicions.[16]



(VACIS gamma-ray image of *sparsely* packed cargo containers)[17]

Integrated Cargo Inspection System

In Hong Kong harbor, Science Applications International Corporation (SAIC, the manufacturer of these non-intrusive scanning devices) is experimenting with three-layered, non-intrusive scanning devices. The three-layered defense – called the Integrated Cargo Inspection System (or ICIS) – is simply the VACIS gamma-ray machine lined together with a radiation portal monitor and an optical character reader to scan container identification numbers. Incoming trucks pass under the monitors at 10 miles per hour while SAIC employees monitor the images of the container contents and save copies.[18]

[15] Fortune 100 estimates that each day that a container is sitting on the docks adds 0.5 percent product value to the cost, Susan Martonosi, et al, "Evaluating the Viability of 100 per cent container inspection at America's Ports," RAND Corp., p. 228, citing C. Spencer, "International Supply Chain Security Regulatory Programs," October 2003.

[16] Susan Martonosi, et al, "Evaluating the Viability of 100 per cent container inspection at America's Ports," RAND Corp., p. 226, citing ARACOR, ARACOR Eagle Product Information, (2004).

[17] Image provided by Advanced Aviaonics & Aviation, Inc., http://interlink17.tripod.com/vechle.html and Defensetech.org, http://www.defensetech.org/archives/002347.html. Densely packed containers may not reveal as much, and even in this image, it could be difficult for an inspector to be able to detect hidden contraband in the wheel barrels and boxes.

[18] SAIC, "Integrated Container Inspection System (ICIS), Hong Kong Demonstration, Frequently Asked Questions," p. 5. Other information in this section was provided by former Customs Assistant Commissioner, John Hensley, presently Vice President SAIC.

Currently, ICIS is simply a pilot program that has been funded by SAIC and tolerated by Hong Kong authorities. In fact, the Hong Kong authorities have insisted that ICIS process trucks and containers at no less than 10 miles per hour out of concern that even one lane of slowed traffic due to inspections is enough to seriously hamper commerce. Further, although pictures of container images are taken by SAIC employees, CBP inspectors have not been able to actually examine the images (although, conceivably, as technology is implemented, images could be sent back to the United States by fiber optic wire to CBP's National Targeting Center for newly developed software to sort and inspectors to examine). These images, too, can only show an inspector so much, and prohibited items can certainly be disguised. From the illegal drug trade, we know, for example, that heroine can be disguised in artwork.[19]

(Drug Enforcement Agency pictures of seized vehicle with illegal drug-related cash and sandals containing heroine)[20]

SAIC estimates that, in order for the same rate of commercial activity at Hong Kong harbor to be maintained, it would require 50 lanes of ICIS machines to run all U.S.-bound containers through the ICIS system, at a cost of $3 million to $4 million per machine. To implement this system at the over 700 foreign ports abroad that import cargo to the United States would be an enormous undertaking.[21] This raises the issue of whether there is even enough dock space at a highly space-scarce port such as Hong Kong's; even if the space could be acquired by an eminent domain process, the cost could be enormous (square footage in Hong Kong is comparable in cost to space in Manhattan).

Where Should Inspections Occur?

Issues such as eminent domain raise the issue of where inspections would be implemented. While implementation of an ICIS-like system overseas carries the advantage of having containers inspected before a potential terrorist threat reaches the

[19] Drug Enforcement Agency report on Operation High Step http://www.dea.gov/pubs/pressrel/pr113005a.html.
[20] http://www.dea.gov/pubs/pressrel/pr111705.html.
[21] An amendment on the Senate Floor to the DHS appropriations bill (H.R. 5441), would require DHS to expand full implementation of the pilot ICIS program to three ports (sec. 571 of the Senate-passed bill).

United States, it also has a number of flaws. First, foreign port inspections depend entirely on cooperation by foreign authorities. Of the over 700 ports that import cargo to the United States, some have very low volume and some may be less willing to have a CBP inspection regime on their soil. Even low-volume ports may raise competing national security issues, however. Therefore, requiring foreign countries to implement ICIS or other 100 percent scanning systems would probably have repercussions for U.S.-based companies. Even in locations that are sympathetic to American security interests, there is an obvious concern for the flow of commerce and the expense of purchasing inspection equipment and stationing CBP personnel abroad.

Also, foreign port container inspections can only attempt to ensure that the containers hold benign cargo as of the time they are inspected. Once the container is on the ship, the container conceivably could be moved to another port, offloaded, and have its contents replaced (and sealed with counterfeit seals), or it may be manipulated at sea.

Some may argue that the United States should inspect all containers when they arrive, but the very obvious problem with inspecting containers at each of 322 U.S. ports of entry[22] is that terrorists can easily detonate a dirty bomb or weapon of mass destruction *at the port facility, before the container is inspected*. Cordoning off inspection areas can have limited mitigating effect and the cost of footprint space can be astronomical, as discussed above. As a practical matter, the containers could only be checked as they are loaded on trains or trucks and sent through an ICIS type inspection, and, as discussed before, this may slow the flow of commerce to suppliers and would probably create a backlog of containers held at port.[23]

It seems evident that the initially "simple" solution for 100 percent inspection becomes very complex and costly to implement,[24] especially when there is a more prudent policy that is no less vigilant.

What Legislation Should Congress Pursue?

In determining strategy, policymakers should keep in mind what the primary objective of port security is. It is to thwart the efforts of terrorists and other evil doers to cause catastrophic disruption to the homeland, whether through weapons of mass destruction *or through crippling of commerce by premature policies*.[25] Instead of

[22] CBP, "Performance and Accountability Report," FY2005, p. 6.
[23] The assessment of the Department of Homeland Security is that ICIS may contribute to future cargo security, but can only supplement inspections at this time. Testimony of Vayl Oxford, Director, Domestic Nuclear Detection Office, Department of Homeland Security, before the House of Representatives Homeland Security Committee, May 25, 2006 ("DHS has sent teams to observe the ICIS pilot and determined that the technology they have has potential, but still faces significant limitations.").
[24] Editorial, "The Right Kind of Security - It's a bad idea to inspect each of the 11 million containers that enter this country every year," *The Washington Post*, June 1, 2006. Editorial, "Schumer's Dubai deal," *The Washington Times*, May 11, 2006.
[25] Booz-Allen-Hamilton has estimated that threats to even certain ports could lead to a national port shut down costing $58 billion. Gerencser, M.J. Weinberg, and D. Vincent, Booz-Allen-Hamilton, "Port

insisting on a policy of 100 percent inspections, Congress should instead support the Department of Homeland Security's efforts to meet its primary objective.

Some policymakers have advocated the use of ICIS as a new technological advance that can implement 100 percent scanning inspection. While the innovation is certainly an important step forward in cargo inspections, the Administration and Congress should continue on its sound policy course of enhancing container inspections in line with cost-benefit analysis. Since 9/11, both the Administration and Congress have pursued judicious use of resources to thwart the terrorist threat coming through U.S. portals from abroad. In applying the same policy towards container security, containers have been inspected in line with the advancement of technology and resources, without hampering American commerce. One hundred percent physical or scanning inspection of cargo containers is a worthy goal, but such a policy should be pursued intelligently and with regard to technological and resource limitations.

In general, the most important policies towards port security that Congress should drive and support include:

- officially authorizing, with general guidelines, initial implementation of a layered approach to cargo inspections (using various inspection methods and utilizing risk assessment);
- supporting DHS as it proceeds to *new* stages in a layered inspection process *as new technology develops*, and as new methods and programs prove useful;
- authorizing the acquisition of more non-intrusive inspection machines, reasonable foot print space at major ports, and funding research and development of new inspection and security technologies. (For example, one promising technology is motion and light detectors that can be embedded in cargo containers and can indicate a penetration. Another example is a second generation of gamma-ray imaging that is in development; and,
- supporting the negotiation of agreements with foreign countries and port authorities to allow DHS inspectors access to containers destined for the United States, and the negotiation of international standards for container seals utilizing the most recent technology. DHS should also further explore security certifications of businesses importing goods from abroad, but it needs to verify those security measures to a reasonable degree as current verification is inadequate.

Other port security programs and policies that Congress should encourage and support include:

- expanding port security pilot programs such as ICIS to willing foreign ports;

Security War Game: Implications for U.S. Supply Chains," 2003 (available at http://www.boozallen.com/publications/article/1440496).

- continuing to improve DHS contingency planning at ports and transportation facilities;
- upgrading minimum standards for security at the same;
- upgrading physical inspection and verification of those security plans;
- completing programs started under MTSA (e.g., identification cards for port facility workers);
- developing new ways to verify and upgrade cargo manifest information sent to DHS in advance;
- providing more resources to send inspectors abroad to provide advance security; and,
- developing more coordination with the intelligence community in obtaining warning information about cargo security threats.

Conclusion

The terrorist attacks of 9/11 have wisely focused the nation's attention on securing the homeland against foreign attack, but policymakers should be both proactive and realistic in the use of resources and avoid providing terrorists a victory by insisting on excessively costly inspections that will risk our economic future. Instead, a sensible response to such terrorist threats is to utilize different layers of screening in line with available technology and resources, and upgrade these processes as new technology, resources, and reduced costs make more inspections feasible. That is the policy that the Administration, with Congress's oversight, has implemented since 9/11. Congress should continue to be supportive of this approach, and it should be vigilant in assuring that port-security policies remain in line with technological improvements.